UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO

JAMES P. BRICKMAN, on behalf of himself and all individuals similarly situated, 7800 1st Street North St. Petersburg, FL 33702 Plaintiffs, v. MAXIMUS, INC. c/o Corporation Service Company 50 West Broad Street, Suite 1330 Columbus, OH 43215 *and* MAXIMUS US SERVICES, INC. c/o Corporation Service Company 50 West Broad Street, Suite 1330 Columbus, OH 43215 Defendants.	Civil Action No.: 2:21-cv-03822 Judge Michael H. Watson Magistrate Judge Kimberly A. Jolson **FIRST AMENDED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff James P. Brickman ("Mr. Brickman" or "Plaintiff"), individually and on behalf of all others similarly situated, through his undersigned counsel, alleges as follows against defendants Maximus, Inc. and Maximus US Services, Inc. (together, "Maximus" or "Defendant"), based upon personal knowledge as to himself and, as to all other matters, upon information and belief, including his counsel's investigation. Plaintiff believes additional evidentiary support exists for his allegations, given an opportunity for discovery.

I. INTRODUCTION

1. Defendant Maximus provides data management services to the Ohio Department of Medicaid ("ODM"), including in relation to credentialing and tax identification of healthcare

providers ("Medicaid Providers").

2. On or around June 18, 2021, Maximus began informing Medicaid Providers, including Mr. Brickman, that it "recently experienced a cybersecurity incident where an actor accessed a Maximus server that involved personal information we received in connection with services that Maximus provides" (the "Data Breach").

3. Maximus disclosed that the following categories of personally identifiable information ("PII") were compromised in the Data Breach: "name, date of birth, Social Security number, and DEA number."

4. Approximately 334,690 Medicaid Providers were affected by the Data Breach.

5. Maximus is responsible for allowing the Data Breach to occur because it failed to implement and maintain reasonable safeguards and failed to comply with industry-standard data security practices as well as federal and state laws and regulations governing deceptive and unfair trade practices and data security.

6. Maximus had obligations created by, among other things, federal and state laws and regulations regarding data security and privacy, industry standards, and common law to keep Medicaid Providers' PII confidential and to protect it from unauthorized access and disclosure.

7. Maximus's data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare and government contracting industries preceding the date of the Data Breach, as well as given the incredibly sensitive nature of PII that it retained on its servers.

8. By obtaining, collecting, and using Mr. Brickman's and class members' PII, Maximus assumed legal and equitable duties and knew or should have known that it was responsible for protecting Mr. Brickman's and class members' PII from disclosure.

9. As a result of Maximus's failure to protect the PII it was entrusted with, Mr.

Brickman's and class members' PII were accessed by malicious cyber criminals.

10. Mr. Brickman and class members therefore are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future.

11. They also suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

12. Mr. Brickman and class members have also lost the inherent value of their PII.

13. Accordingly, Mr. Brickman brings this action against Maximus seeking redress for its unlawful conduct and asserting claims for negligence, negligence *per se*, declaratory judgment, breach of confidence, breach of contract, and violations of the Florida Deceptive and Unfair Trade Practices Act.

II. PARTIES

A. *Plaintiff James P. Brickman*

14. Mr. Brickman is a natural person who resides in and is a citizen of Saint Petersburg, Florida.

15. Prior to moving to Florida in or around 2004, Mr. Brickman was a resident of the State of Ohio.

16. Mr. Brickman was certified as a Registered Nurse (RN) in Ohio in or around 1985. He was certified as a Certified Registered Nurse Anesthetist (CRNA) in or around 1999. Mr. Brickman maintains and has maintained his Ohio licensure and certification through the present.

17. In order to become an RN and/or a CRNA, Mr. Brickman had to go through the credentialing process to become a Medicaid Provider.

18. Through this credentialing process, Mr. Brickman provided various PII, including his name, date of birth, Social Security Number, and DEA (Drug Enforcement Administration) number.

19. This information was later provided to Maximus.

20. Mr. Brickman entrusted PII and other confidential information to Maximus (through the Medicaid credentialing process described above) with the reasonable expectation and understanding that any contractor who obtained possession of such PII, including Maximus, would protect, maintain, and safeguard that information from compromise, unauthorized disclosure, and misuse by unauthorized actors.

21. On or about June 18, 2021, Mr. Brickman received correspondence from Maximus confirming the Data Breach, and noting that his name, date of birth, Social Security number, and DEA number had been compromised in the data breach (the "Notice").[1]

22. As a result of Mr. Brickman's PII being exposed in the Data Breach, Mr. Brickman has spent approximately 1-2 hours reviewing information related to his credit reports to monitor for fraudulent activity and to sign up for credit monitoring services.

23. He will continue to monitor his banking and financial statements and credit history for abnormal activity into the indefinite future as a result of the significant risk of fraud and identity theft he faces as a result of the Data Breach.

24. He is also spending time considering whether to implement a credit freeze to prevent against future instances of identity theft.

[1] A copy of this Notice is attached hereto as Exhibit A.

25. Mr. Brickman also faces an increased risk that someone may use his DEA number to impersonate him for the purposes of billing ODM for services or for writing prescriptions. This unique risk further exacerbates the risk of identity theft posed by the compromise of his Social Security number.

26. If Mr. Brickman discovers any misuse of his DEA number to illegally prescribe or obtain prescription drugs, he will be forced to file a report with his local police department and report such activity to the DEA Diversion Control Division.

27. Mr. Brickman has not previously been a victim of fraud or identity theft, other than unrelated instances in which his credit card information was stolen, and he is not aware of any prior compromise of his Social Security Number or DEA number in a prior data breach incident.

28. As a consumer concerned with the privacy of his personal information, Mr. Brickman has taken considerable steps to protect his identity and maintain his privacy prior to the Data Breach and since the Data Breach.

29. Mr. Brickman has refrained from transmitting unencrypted PII over the internet or any other unsecured source.

30. Mr. Brickman also stores any and all documents containing his PII in a safe and secure physical location, and destroyed (primarily by shredding such documents) any documents he receives in the mail that contain any of his PII, or that may contain any information that could otherwise be used to steal his identity.

B. *Defendant Maximus, Inc.*

31. Maximus, Inc. is a corporation incorporated in the state of Virginia. Its headquarters is located at 1891 Metro Center Drive, Reston, Virginia 20190.

32. Maximus operates through a number of wholly-owned subsidiaries, including Defendant Maximus US Services, Inc.

C. Defendant Maximus US Services, Inc.

33. Maximus US Services, Inc. is a corporation incorporated in the state of Indiana. Its headquarters is located at 1891 Metro Center Drive, Reston, Virginia 20190.

34. On or about September 11, 2019, Maximus US Services, Inc. entered into a contract with the State of Ohio, through the Department of Administrative Services on behalf of ODM, to provide a solution known as Ohio Medicaid Enterprise System ("OMES"), Provider Network Management (the "Contract").[2] The Ohio Medicaid Enterprise System refers to ODM and other state agencies that participate in Medicaid and related program operations.

35. Pursuant to the Contract, Maximus US Services, Inc. is responsible for collecting and processing a vast array of data on Medicaid Providers credentialed by ODM. These services include automated eligibility determination processes including screening, certification, and credentialing. They also include Provider Information Management services, which cover maintenance of the OMES Provider Registry, the system of record for provider information used throughout OMES in support of operational processing of all OMES functions.

36. Maximus was and is principally responsible for the design, development, maintenance, and operation of these systems and servers used to collect, store, and process Medicaid Providers' PII.

37. Although Maximus, Inc. provided notice of the Data Breach, Mr. Brickman understands that the contract with ODM was entered into by Maximus US Services, Inc., as described above. Mr. Brickman is not privy to Maximus's internal corporate structure or how it allocates work among its various affiliates and subsidiaries. This information is solely within the

[2] Ohio Procurement, Current Contract Detail: OMES Provider Network Management, *available at* https://web.archive.org/web/20210423221548/https://procure.ohio.gov/proc/viewContractsAwards.asp?contractID=36708 (last visited September 28, 2021).

possession of Maximus. Accordingly, for the purposes of this Complaint, Mr. Brickman raises his allegations against both entities (collectively referred to as Maximus), subject to discovery to determine which Maximus entity or entities should be held liable for the unlawful conduct alleged herein.

III. JURISDICTION AND VENUE

38. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because putative class members are citizens of a different state than Defendants.

39. This Court has personal jurisdiction over Maximus because it is authorized to conduct and does regularly conduct business in Ohio.

40. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Mr. Brickman's and class members' claims occurred in this District. ODM, which retained the services of Maximus, is located in this district. All of the members of the class went through a credentialing process administered by ODM, which contracted with Maximus to maintain their PII.

IV. COMMON FACTUAL ALLEGATIONS

A. Maximus's Knowledge That It Was and Is a Target of Cyber Threats

41. Maximus knew it was a prime target for hackers given the significant amount of sensitive PII processed through its computer data and storage systems, including the server(s) compromised in the Data Breach.

42. As alleged above, Maximus processed highly sensitive PII for Medicaid Providers, including names, dates of birth, Social Security numbers, and DEA numbers, in relation to

credentialing and tax verification purposes for ODM.

43. Experts studying cyber security routinely identify entities in the healthcare industry, as well as government contractors, as being particularly vulnerable to cyberattacks because of the value of the PII that they collect and maintain.

44. Maximus's knowledge is underscored by the massive number of data breaches, including those perpetrated against the healthcare sector, that have occurred in recent years.

45. According to a report from cloud security company Bitglass, in 2020, data breaches in the healthcare industry rose 55.1% from 2019, totaling 599 data breaches affecting more than 26 million people.[3]

46. According to a 2018 report from cybersecurity firm BitSight regarding data breaches affecting government contractors, 4.3 percent of government contractors in the technology space reported at least one data breach since 2016, and government contractors in the healthcare space reported the highest number of data breaches – with 8 percent of such contractors reporting a data breach since 2016.[4]

47. Indeed, Maximus itself has acknowledged past attempts to breach its systems, writing that "[w]e are a trusted provider to government and other clients of critical health and human services that rely heavily upon technology systems, software and networks to receive, input, maintain and communicate participant and client data. Although we have experienced occasionally attempted security breaches, to our knowledge, none of those attempts have been

---

[3] Anuja Vaidya, *Report: Healthcare data breaches spiked 55% in 2020*, MedCityNews (Feb. 17, 2021), https://medcitynews.com/2021/02/report-healthcare-data-breaches-spiked-55-in-2020/ (last visited September 27, 2021).

[4] Derek B. Johnson, *How vulnerable are contractors when it comes to data breaches?* (Feb. 16, 2018), https://fcw.com/articles/2018/02/15/contractor-data-breach-report.aspx (last visited September 27, 2021)

successful."[5]

48. Maximus further acknowledged that "[t]he risk of a security breach, system disruption, ransom-ware attack or similar cyber-attack or intrusion, including by computer hackers, cyber terrorists or foreign governments, is persistent and substantial as the volume, intensity and sophistication of attempted attacks, intrusions and threats from around the world increase daily."[6]

49. Despite knowing the prevalence of data breaches targeting companies in the healthcare and government contracting sectors, including knowledge of attempts against Maximus's own servers, Maximus failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to its highly sensitive systems and databases. Maximus had the resources to prevent a breach, but it neglected to adequately invest in data security, despite the growing number of well-publicized data breaches and its own knowledge of prior attempted attacks against its own systems.

50. Maximus failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures to ensure that similar vulnerabilities were avoided or remedied and that Mr. Brickman's and class members' PII were protected.

51. Due to Maximus's failure to conform to the accepted industry practices and standards of data security and protection measures, Mr. Brickman's and the class members' PII was disclosed and misappropriated to the public and unauthorized third parties.

52. Further, based on information and belief, Maximus had knowledge and was aware that its data security measures and protections did not meet the accepted industry practices and

[5] Maximus, Inc., Form 10-K (Sep. 30, 2020), https://www. https://www.sec.gov/Archives/edgar/data/0001032220/000103222020000102/mms-20200930.htm (last visited September 27, 2021)
[6] *Id.*

standards to properly protect Mr. Brickman's and the class members' PII from disclosure to the public and unauthorized third parties.

B. The Data Breach

53. On or around June 18, 2021, Maximus began informing Medicaid Providers, including Mr. Brickman, that it "recently experienced a cybersecurity incident where an actor accessed a Maximus server that involved personal information we received in connection with services that Maximus provides."[7]

54. Maximus stated that "[o]n My 19, 2021, Maximus learned that a Maximus server that contained personal information provided to the Ohio Department of Medicaid (ODM) or to a Managed Care Plan for purposes of credentialing or tax identification in [the Medicaid Providers'] role as a healthcare provider was accessed by an unknown party." According to Maximus, "the server was impermissibly accessed starting on May 17, 2021."

55. Maximus disclosed that the following categories of Medicaid Providers' personally identifiable information ("PII") was compromised in the Data Breach: "name, date of birth, Social Security number, and DEA number."

56. Approximately 334,690 Medicaid Providers had their PII compromised in the Data Breach.

57. Maximus is responsible for allowing the Data Breach to occur because it failed to implement and maintain reasonable safeguards and failed to comply with industry-standard data security practices as well as federal and state laws and regulations governing data security.

58. During the duration of the Data Breach, Maximus failed to, among other things, detect that ill-intentioned criminals had accessed its server(s), notice the massive amounts of data

[7] *See* Exhibit A.

that were compromised, or take any steps prior to or during the Data Breach to investigate the red flags that should have warned Maximus that its systems were not secure.

59. Had Maximus properly monitored its information technology infrastructure, it would have prevented or mitigated the scope and impact of the Data Breach.

60. Maximus had obligations created by, among other things, federal and state laws and regulations regarding data security and privacy, industry standards, and common law to keep Medicaid Providers' PII confidential and to protect it from unauthorized access and disclosure.

61. Mr. Brickman and class members provided their PII to Maximus (via ODM or a Managed Care Plan) with the reasonable expectation and mutual understanding that Maximus would comply with its obligations to keep such information confidential and secure from unauthorized access.

62. Maximus's data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare and government contracting industries preceding the date of the Data Breach, as well as given the incredibly sensitive nature of PII that it retained in its servers.

63. By obtaining, collecting, and using Mr. Brickman's and class members' PII, Maximus assumed legal and equitable duties and knew or should have known that it was responsible for protecting Mr. Brickman's and class members' PII from disclosure.

64. As a result of Maximus's failure to protect sensitive PII it was entrusted with, Mr. Brickman and class members are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future.

65. Mr. Brickman and class members have also lost the inherent value of their PII.

C. Maximus Failed to Comply with Statutory and Regulatory Obligations.

66. Maximus had obligations created by the Federal Trade Commission Act ("FTC

Act"), 15 U.S.C. § 45, industry standards, state law, and common law to keep Mr. Brickman's and class members' PII confidential and to protect it from unauthorized access and disclosure.

67. Maximus was prohibited by the FTC Act from engaging in "unfair or deceptive acts or practices in or affecting commerce."

68. The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

69. Moreover, federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For example, the FTC has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[8]

70. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[9] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the

[8] *Start with Security, A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 23, 2021).

[9] *Protecting Personal Information, A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 23, 2021).

system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[10]

71. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[11]

72. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[12]

73. Maximus also failed to comply with commonly accepted industry standards for data security. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

---

[10] *Id.*
[11] *Start with Security*, *supra* n. 8.
[12] *Privacy and Security Enforcement: Press Releases*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited June 23, 2021)

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

74. Maximus is also required by various states' laws and regulations to protect Mr. Brickman's and class members' PII and to handle any breach of the same in accordance with applicable breach notification statutes.

75. In addition to its obligations under federal and state laws, Maximus owed a duty to Mr. Brickman and class members whose PII was entrusted to Maximus to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

76. Maximus owed a duty to Mr. Brickman and class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its systems and networks adequately protected the PII of Mr. Brickman and class members.

77. Maximus owed a duty to Mr. Brickman and class members whose PII was entrusted to Maximus to design, maintain, and test its systems to ensure that the PII in Maximus's possession was adequately secured and protected.

78. Maximus owed a duty to Mr. Brickman and class members whose PII was entrusted to Maximus to create and implement reasonable data security practices and procedures to protect the PII in its possession.

79. Maximus owed a duty to Mr. Brickman and class members whose PII was entrusted to Maximus to implement processes that would detect a breach on its data security systems in a timely manner.

80. Maximus owed a duty to Mr. Brickman and class members whose PII was entrusted to Maximus to act upon data security warnings and alerts in a timely fashion.

81. Maximus owed a duty to Mr. Brickman and class members whose PII was entrusted to Maximus to disclose if its systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust PII to Maximus.

82. Maximus owed a duty to Mr. Brickman and class members whose PII was entrusted to Maximus to disclose in a timely and accurate manner when data breaches occurred.

83. Maximus owed a duty of care to Mr. Brickman and class members because they were foreseeable and probable victims of any inadequacy in its affirmative development of the systems to maintain PII and in its affirmative maintenance of those systems.

84. In this case, Maximus was fully aware of its obligation to use reasonable measures to protect the PII of its members. Maximus also knew it was a target for hackers. But despite understanding the consequences of inadequate data security, Maximus failed to comply with industry-standard data security requirements.

85. Maximus's failure to employ reasonable and appropriate measures to protect against unauthorized access to its members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, and various state consumer protection and data breach statutes.

D. The Value of PII and Effects of the Data Breach

86. It is well known that PII, including Social Security numbers, is a highly valued commodity and a frequent target of hackers.

87. According to Javelin Strategy & Research, in 2017 alone over 16.7 million

individuals were affected by identity theft, causing $16.8 billion to be stolen.[13]

88. Consumers place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes significant negative financial impact on victims as well as severe distress and other strong emotions and physical reactions.

89. Consumers are particularly concerned with protecting the privacy of their Social Security numbers, which is the "secret sauce" that is "as good as your DNA to hackers."[14]

90. There are long-term consequences to data breach victims whose Social Security numbers are taken and used by hackers.

91. Even if they know their Social Security numbers have been accessed, Mr. Brickman and class members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start."[15] And "[f]or some victims of identity theft, a new number actually creates new problems. If the old credit information isn't associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[16]

92. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name, but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the

---

[13] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), *available at* https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin (last visited June 23, 2021).

[14] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), *available at* https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html (last visited June 23, 2021).

[15] Social Security Admin., Identity Theft and Your Social Security Number, at 6-7, *available at* https://www.ssa.gov/pubs/EN-05-10065.pdf (last visited June 23, 2021).

[16] *Id.*

victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, seek unemployment or other benefits, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

93. PII is such a valuable commodity to identity thieves that, once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

94. There is a strong probability that entire batches of stolen information have been dumped on the black market and will be again in the future, meaning Mr. Brickman and class members are at an increased risk of fraud and identity theft for many years to come.

95. Thus, Mr. Brickman and class members must vigilantly monitor their credit reports, financial accounts, and other areas of concern for the foreseeable future.

96. There may be a significant time lag between when PII is stolen and when it is actually misused.

97. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

98. Accordingly, the two years of credit monitoring that Maximus offered victims of the Data Breach is woefully inadequate to guard against the risks they face.

99. And, in any event, the two years of credit monitoring that Maximus offered victims

[17] U.S. Government Accountability Office, *Report to Congressional Requesters* (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited June 23, 2021)

of the Data Breach does nothing to compensate them for the damages they suffered as a result of the Data Breach.

100. The risk of identity theft is particularly acute where detailed personal information is stolen, such as the PII that was compromised in the Data Breach.

101. The cyber black-market demonstrates that PII is a valuable property right.[18] Moreover, its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts, which include heavy prison sentences. This obvious risk/reward analysis illustrates that PII has considerable market value.

102. The value of PII is underscored by the growing number of legitimate marketplaces allowing consumers to monetize their PII.[19]

103. As the result of the Data Breach, Mr. Brickman and class members have suffered or will suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. identity theft and fraud resulting from theft of their PII;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their online accounts, including financial accounts;

c. losing the inherent value of their PII;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. unauthorized access to and misuse of their online accounts;

---

[18] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[19] *Markets for personal data*, Project VRM, Harvard University, https://cyber.harvard.edu/projectvrm/VRM_Development_Work#Markets_for_personal_data (last visited June 23, 2021).

f. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

g. lowered credit scores resulting from credit inquiries following fraudulent activities;

h. costs associated with time spent and the loss of productivity or enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, addressing other varied instances of identity theft – such as credit cards, bank accounts, loans, government benefits, and other services procured using the stolen PII, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach;

i. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or more unauthorized third parties; and

j. continued risk of exposure to hackers and thieves of their PII, which remains in Maximus's possession and is subject to further breaches so long as Maximus fails to undertake appropriate and adequate measures to protect Mr. Brickman and class members.

104. Additionally, Mr. Brickman and class members place significant value in data security. According to a survey conducted by cyber-security company FireEye, approximately

50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[20]

105. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[21] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII to bad actors—would be much higher today.

106. Mr. Brickman and class members are at an imminent risk of fraud, criminal misuse of their PII, and identity theft for years to come as result of the Data Breach and Maximus's deceptive and unconscionable conduct.

E. The DEA Numbers and Effect of Their breach.

107. Mr. Brickman and class members also face the nightmare scenario of unauthorized actors using their DEA numbers to illegally write prescriptions for controlled substances.

108. Any person that prescribes or dispenses controlled substance must register with the DEA and obtain a DEA number.[22]

---

[20] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://www.fireeye.com/blog/executive- perspective/2016/05/beyond_the_bottomli.html (last visited June 23, 2021).

[21] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at 17, Oct. 2002, *available at* https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf

[22] DEA Diversion Control Division, Part 1301 – Registration of Manufacturers, Distributors, and

109. An individual's DEA number is not publicly available and is the only confidential component that must be included on a medical practitioner's prescription for a controlled substance.[23]

110. The registration process for an individual to obtain a DEA number is extensive and requires submission of professional licenses, certifications, and payment of a registration fee.

111. Thus, Mr. Brickman and the putative class have previously undertaken the time consuming and expensive task of obtaining a DEA number, which presently costs approximately $888.[24]

112. Stolen DEA numbers pose a real threat to prescriber victims such as Mr. Brickman, particularly in light of the ongoing opioid abuse epidemic. According to a recent survey conducted by the healthcare IT security company Imprivata, "about 10% of prescribers admit to having their DEA number stolen, or compromised," and "29% of the prescribers know a colleague who has fallen prey to DEA number fraud." And, as to the risk posed by such theft, Imprivata notes that "[a] stolen DEA number can lead to hundreds if not thousands of fraudulent prescriptions."[25]

113. The theft of prescribing information, such as DEA numbers, is not a new phenomenon. It has been widely reported, and so Maximus was or should have been aware of the

---

Dispensers of Controlled Substances, 21 CFR 1301.11, *available at* https://www.deadiversion.usdoj.gov/21cfr/cfr/1301/1301_11.htm (last visited Sept. 22, 2021)

[23] See Issuing a Valid Prescription: What Every Prescriber Needs to Know, *available at* https://www.pharmacy.ohio.gov/Documents/Pubs/Special/DangerousDrugs/Issuing%20a%20Valid%20Prescription%20-%20What%20Every%20Prescriber%20Needs%20to%20Know.pdf (last visited Sept. 22, 2021)

[24] See Diversion Control Division, Part 1301 – Registration of Manufacturers, Distributors, and Dispensers of Controlled Substances, *available at* https://www.deadiversion.usdoj.gov/21cfr/cfr/1301/1301_13.htm#feeCategories (last visited Sept. 22, 2021).

[25] *Protect against DEA number theft with Electronic Prescribing of Controlled Substances*, IMPRIVATA, available at https://www.imprivata.com/sites/imprivata/files/resource-files/CID-DS-DEAtheft-0318.pdf (last visited September 23, 2021).

risk posed by such theft.

114. For example, in 2011, the New York Times reported that the New York Health Department's Bureau of Narcotic Enforcement had "identified a large nationwide organized crime gang known to traffic in illicit and legal drugs as being involved in the distribution of stolen prescription forms."[26]

115. Similarly, the Department of Justice's National Drug Intelligence Center's 2009 National Drug Threat Assessment reported that "[p]rescription drug distributors and abusers typically acquire Schedule II prescription drugs through . . . [inter alia,] prescription fraud by theft of prescription pads or by computer-created prescription pads."[27]

116. And according to a 2014 report from the Department of Justice and the Center for Problem-Oriented Policing, "Prescription drug fraud can take many forms. The most common tactics are[, inter alia,] to forge or alter a prescription . . . and to phone in fraudulent prescriptions posing as a doctor's office employee" – steps which require access to a prescriber's DEA number.[28]

117. The Centers for Medicare and Medicaid Services also highlighted the risk of DEA number theft in its April 2006 Prescription Drug Benefit Manual: "Prescription pads and/or DEA numbers can be stolen from prescribers. This information could illegally be used to write prescriptions for controlled substances or other medications often sold on the black market."[29]

---

[26] Thomas Kaplan, *State Investigates Thefts of Prescription Pads at Hospitals*, N.Y. TIMES (Oct. 24, 2011), https://www.nytimes.com/2011/10/24/nyregion/prescription-pads-stolen-from-new-york-city-hospitals.html (last visited September 23, 2021).

[27] *National Drug Threat Assessment 2009*, NAT'L DRUG INTELLIGENCE CTR., (Dec. 2008), https://www.justice.gov/archive/ndic/pubs31/31379/pharm.htm (last visited September 23, 2021).

[28] Julie Wartell & Nancy G. La Vigne, *Prescription Drug Fraud and Misuse*, CTR. FOR PROBLEM-ORIENTED POLICING 11 (Apr. 2013), https://cops.usdoj.gov/RIC/Publications/cops-p257-pub.pdf (last visited September 23, 2021).

[29] *Prescription Drug Benefit Manual Chapter 9 – Part D Program to Control Fraud, Waste and Abuse*, CTRS. FOR MEDICARE & MEDICAID SERVS. 59 (Apr. 25, 2006), https://www.hhs.gov/guidance/sites/default/files/hhs-guidance-documents/pdbmanual_chapter9_fwa_10.pdf (last visited September 23, 2021)

118. The Ohio Board of Pharmacy explained in an "Important Notice to All Licensees Regarding Fraudulent Prescriptions" how the theft of a DEA number enables prescription drug fraud:

> Phone-in prescriptions: suspects will download apps to generate VoIP phone numbers which are then used to impersonate prescribers and fictitious patients. The suspects then call pharmacies and order promethazine/codeine, accompanied with a non-controlled substance such as Flonase, an inhaler, prednisone, or antibiotic. **The suspect provides a DEA number**, and NPI number, and in many instances a diagnosis code. The caller also provides a generated number for the "patient." Unsuspecting pharmacies then call the "patient" once the prescription is filled, and the "patient" typically tells the pharmacy that a relative will pick it up. Pharmacies sometimes call the number left for the prescriber to verify that the prescription is valid, and they end up speaking with the suspect again.[30]

119. As the foregoing illustrates, there is a market for stolen DEA numbers. And cybercriminals are taking advantage of this market. For example, in 2019, the pharmaceutical company Akorn Inc. had its data sold on the black market by a "hacker who [was] offering to sell the data to the highest bidder or back to the company." The database included "business related information, including DEA numbers."[31]

120. In the event that Mr. Brickman's DEA number was illegally used, Mr. Brickman would be forced to spend time reporting the misuse to his local police department and to the DEA Diversion Control Division directly.

121. Further, Mr. Brickman would be required to spend extensive time and effort participating in and responding to the ensuing law enforcement investigation.

---

[30] *Important Notice to All Licensees Regarding Fraudulent Prescriptions – UPDATED*, State of Ohio Board of Pharmacy, available at https://www.pharmacy.ohio.gov/Documents/Pubs/Newsletter/2020/Important%20Notice%20to%20All%20Licensees%20Regarding%20Fraudulent%20Prescriptions%20-%20UPDATED.pdf (last visited September 23, 2021) (emphasis added).

[31] Steve Ragan, *Akorn Inc. has customer database stolen, records offered to highest bidder*, CSO Online (June 18, 2015), https://www.csoonline.com/article/2938032/akorn-inc-has-customer-database-stolen-records-offered-to-highest-bidder.html (last visited September 23, 2015)

122. Misuse of a DEA number would require issuance of a new DEA number which requires a time consuming application process, submission of licenses and certifications, payment of a fee of approximately $888, and the prescriber would not be able to write prescriptions requiring a DEA number during the time period upon which they were waiting for a new DEA number to be issued.[32]

123. Additionally, if Mr. Brickman's DEA number is misused to illegally prescribe or obtain prescription drugs, he may also face the reality of being forced to defend against criminal charges for violations of the Controlled Substances Act and/or face the prospect of being stripped of his licensing and DEA privileges.

124. Further, the credit monitoring offered by Defendants does not address Defendants' exposure of the victims' DEA numbers nor do the Defendants provide any service that the victims can use to track the use of their DEA numbers.

125. Indeed, the credit monitoring offered by Maximus fails entirely to address the legal ramifications that Mr. Brickman and the putative class face if their DEA numbers are used to illegally prescribe or obtain prescription drugs.

V. CLASS ACTION ALLEGATIONS

126. Pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2), and (b)(3), Mr. Brickman seeks certification of the following nationwide class:

> **Nationwide Class:** All residents of the United States of America whose PII was compromised in the Data Breach.

127. The Nationwide Class asserts claims against Maximus for negligence (Count I), negligence *per se* (Count II), declaratory judgment (Count III), breach of confidence (Count IV),

[32] Diversion Control Division, *supra* note 24.

and breach of contract (Count V).

128. Pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2), and (b)(3), Mr. Brickman seeks certification of Florida state claims in the alternative to the nationwide claims, as well as certification of claims for violations of the Florida Deceptive and Unfair Trade Practices Act (Count VI) on behalf of a subclass of Florida residents, defined as follows:

> **Florida Subclass:** All residents of Florida whose PII was compromised in the Data Breach.

129. The Nationwide Class and the Florida Subclass are collectively referred to herein as the "Class."

130. Excluded from the Class are Maximus, any entity in which Maximus has a controlling interest, and Maximus's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, members of their judicial staff, and any judge sitting in the presiding court system who may hear an appeal of any judgment entered.

131. **Risk of Inconsistent or Varying Adjudications. Fed. R. Civ. P. 23(b)(1).** As the proposed Class includes hundreds of thousands of members, there is significant risk of inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for Maximus. For example, injunctive relief may be entered in multiple cases, but the ordered relief may vary, causing Maximus to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which it will comply. Class action status is also warranted because prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to

protect their interests.

132. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. Maximus has admitted that at least 334,690 individuals were victims of the Data Breach.

133. **Commonality and Predominance. Fed. R. Civ. P. 23(a)(2) and (b)(3).** This action involves common questions of law and fact that predominate over any questions affecting individual class members. The common questions include, but are not limited to:

a. Whether Maximus knew or should have known that its computer and data storage systems were vulnerable to attack;

b. Whether Maximus failed to take adequate and reasonable measures to ensure its computer and data systems were protected;

c. Whether Maximus owed a duty of care to Mr. Brickman and class members, as alleged above;

d. Whether Maximus breached the duties of care it owed to Mr. Brickman and class members;

e. Whether Maximus failed to take available steps to prevent and stop the Data Breach from happening;

f. Whether Maximus failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard PII;

g. Whether Maximus's failure to secure Mr. Brickman's and class members' PII in the manner alleged violated federal, state, and local laws and regulations, or industry standards;

h. Whether Maximus was negligent in establishing, implementing, and following

security protocols;

i. Whether Mr. Brickman's and class members' PII was compromised and exposed as a result of the Data Breach and the extent of that compromise and exposure;

j. Whether Maximus's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unauthorized access to, compromise, and/or theft of Mr. Brickman's and class members' PII;

k. Whether Maximus's conduct amounted to violations of state statutes, as alleged below;

l. Whether, as a result of Maximus's conduct, Mr. Brickman and class members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

m. Whether, as a result of Maximus's conduct, Mr. Brickman and class members are entitled to injunctive, equitable, declaratory and/or other relief and, if so, the nature of such relief;

n. Whether Mr. Brickman and class members are entitled to compensatory damages;

o. Whether Mr. Brickman and class members are entitled to punitive damages; and

p. Whether Mr. Brickman and class members are entitled to statutory damages.

134. **Typicality. Fed. R. Civ. P. 23(a)(3).** Mr. Brickman's claims are typical of other class members' claims because Mr. Brickman and class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

135. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Mr. Brickman

is an adequate representative of the Class. Mr. Brickman is a member of the Class. Mr. Brickman has no conflicts of interest with the Class. Mr. Brickman has retained counsel competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation and consumer protection claims. Mr. Brickman intends to vigorously prosecute this case and will fairly and adequately protect the interests of the Class.

136. **Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2).** Class certification is also appropriate under Rule 23(b)(2). Maximus, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole. Moreover, Maximus continues to maintain its inadequate security practices, retains possession of Mr. Brickman's and class members' PII, and has not been forced to change its practices or to relinquish PII by nature of other civil suits or government enforcement actions, thus making injunctive and declaratory relief a live issue and appropriate to the Class as a whole.

137. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs and class members may not be sufficient to justify individual litigation. Here, the damages suffered by Mr. Brickman and the class members are relatively small compared to the burden and expense required to individually litigate their claims against Maximus, a sophisticated financial institution, and thus, individual litigation to redress Maximus's wrongful conduct would be impracticable. Individual litigation by each class member would also strain the court system. Moreover, individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single

adjudication, economies of scale, and comprehensive supervision by a single court.

VI. CAUSES OF ACTION

COUNT I

NEGLIGENCE

(On behalf of Plaintiff and the Nationwide Class or, in the alternative, on behalf of Plaintiff and the Florida Subclass)

138. Mr. Brickman repeats the allegations in paragraphs 1 – 137 of this Complaint, as if fully alleged herein.

139. Maximus owed a duty of care to Mr. Brickman and class members to use reasonable means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems, as alleged herein.

140. These common law duties existed because Mr. Brickman and class members were the foreseeable and probable victims of any inadequate security practices in Maximus's affirmative development and maintenance of its data security systems.

141. In fact, not only was it foreseeable that Mr. Brickman and class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Maximus knew that it was more likely than not Mr. Brickman and other class members would be harmed by such exposure and theft of their PII.

142. Maximus's duties to use reasonable security measures also arose as a result of the special relationship that existed between Maximus, on the one hand, and Mr. Brickman and class members, on the other hand.

143. This special relationship arose because Mr. Brickman and class members entrusted Maximus with their PII, through ODM or a Managed Care Plan, as part of a process of obtaining

credentialing or tax verification required by the Ohio Department of Medicaid.

144. Maximus alone could have ensured that its data security systems and practices were sufficient to prevent or minimize the Data Breach.

145. Maximus's duties to use reasonable data security measures also arose under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII.

146. Various FTC publications and data security breach orders further form the basis of Maximus's duties.

147. In addition, individual states have enacted statutes based on the FTC Act (some of which specifically incorporate the FTC Act's relevant duties), such as the Florida Deceptive and Unfair Trade Practices Act, that also created a duty.

148. Maximus breached the aforementioned duties when it failed to use security practices that would protect the PII provided to it by Mr. Brickman and class members, thus resulting in unauthorized exposure and third party access to Mr. Brickman's and class members' PII.

149. Maximus further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Mr. Brickman's and class members' PII within its possession, custody, and control.

150. As a direct and proximate cause of Maximus's failure to adequately develop and maintain its data security systems, and its failure to use appropriate security practices, Mr. Brickman's and class members' PII was exposed, disseminated, and made available to unauthorized third parties.

151. Maximus admitted that Mr. Brickman's and class members' PII was wrongfully disclosed and accessed as a result of the Data Breach.

152. The Data Breach caused direct and substantial damages to Mr. Brickman and class members, as well as the likelihood of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of credit fraud and identity theft.

153. By engaging in the foregoing acts and omissions, Maximus committed the common law tort of negligence.

154. For all the reasons stated above, Maximus's conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately limit access to and protect the PII; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Mr. Brickman's and class members' PII.

155. But for Maximus's wrongful and negligent breach of its duties owed to Mr. Brickman and class members, their PII would not have been compromised.

156. Neither Mr. Brickman nor class members contributed to the Data Breach or subsequent misuse of their PII as described in this Complaint.

157. As a direct and proximate result of Maximus's negligence, Mr. Brickman and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, DEA number monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by

Maximus, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT II

***NEGLIGENCE* PER SE**

(On behalf of Plaintiff and the Nationwide Class or, in the alternative, on behalf of Plaintiff and the Florida Subclass)

158. Mr. Brickman repeats the allegations in paragraphs 1 – 137 of this Complaint, as if fully alleged herein.

159. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Maximus of failing to use reasonable measures to protect PII.

160. Various FTC publications and orders also form the basis of Maximus's duty.

161. Maximus violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards.

162. Maximus's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Maximus's systems.

163. Maximus's violation of Section 5 of the FTC Act (and similar state statutes, such as the Florida Deceptive and Unfair Trade Practices Act) constitutes negligence *per se*.

164. Mr. Brickman and class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

165. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against.

166. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of defendants' failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Mr. Brickman and class members.

167. As a direct and proximate result of Maximus's negligence, Mr. Brickman and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, DEA number monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Maximus, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT III

DECLARATORY JUDGMENT

(On behalf of Plaintiff and the Nationwide Class or, in the alternative, on behalf of Plaintiff and the Florida Subclass)

168. Mr. Brickman repeats the allegations in paragraphs 1 – 137 of this Complaint, as if fully alleged herein.

169. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., the Court is

authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief.

170. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

171. An actual controversy has arisen in the wake of the Data Breach regarding Maximus's present and prospective common law and other duties to reasonably safeguard its users' PII, and whether Maximus is currently maintaining data security measures adequate to protect Mr. Brickman's and class members from further data breaches that compromise their PII.

172. Mr. Brickman and class members remain at imminent risk that further compromises of their PII will occur in the future.

173. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Maximus continues to owe a legal duty to secure users' PII under the common law, Section 5 of the FTC Act, and various state statutes; and

b. Maximus continues to breach this legal duty by failing to employ reasonable measures to secure Mr. Brickman's and class members' PII.

174. The Court also should issue corresponding prospective injunctive relief pursuant to 28 U.S.C. § 2202, requiring Maximus to employ adequate security practices consistent with law and industry standards to protect its users' PII.

175. If an injunction is not issued, Mr. Brickman and class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Maximus.

176. The risk of another such breach is real, immediate, and substantial.

177. If another breach occurs, Mr. Brickman and class members will not have an

adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

178. The hardship to Mr. Brickman and class members if an injunction does not issue exceeds the hardship to Maximus if an injunction is issued.

179. Among other things, if another data breach occurs at Maximus, Mr. Brickman and class members will likely be subjected to fraud, identify theft, and other harms described herein.

180. On the other hand, the cost to Maximus of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Maximus has a pre-existing legal obligation to employ such measures.

181. Issuance of the requested injunction will not disserve the public interest.

182. To the contrary, such an injunction would benefit the public by preventing another data breach at Maximus, thus eliminating additional injuries that would result to Mr. Brickman, class members, and the hundreds of thousands of other individuals for whom Maximus stores and processes PII, and whose PII would be further compromised.

COUNT IV

BREACH OF CONFIDENCE

(On behalf of Plaintiff and the Nationwide Class or, in the alternative, on behalf of Plaintiff and the Florida Subclass)

183. Mr. Brickman repeats the allegations in paragraphs 1 – 137 of this Complaint, as if fully alleged herein.

184. At all times during Mr. Brickman's and class members' interactions with Maximus, Maximus was fully aware of the confidential and sensitive nature of Mr. Brickman's and class members' PII.

185. As alleged herein and above, Maximus's relationship with Mr. Brickman and class

members was governed by terms and reasonable expectations that Mr. Brickman's and class members' PII would be collected, stored, and protected in confidence, and would not be disclosed to the public or any unauthorized third parties.

186. Mr. Brickman and the class members provided their respective PII to Maximus with the reasonable expectation that Maximus would treat that PII with the same level of confidentiality as PII provided to and held by a bank.

187. Mr. Brickman and the class members provided their respective PII to Maximus (through ODM and/or a Managed Care Plan) with the explicit and implicit understandings that Maximus would protect and not permit their PII to be disseminated to the public or any unauthorized parties.

188. Mr. Brickman and the class members also provided their respective PII to Maximus with the explicit and implicit understandings that Maximus would take precautions to protect the PII from unauthorized disclosure, such as following basic principles of encryption and information security practices.

189. Indeed, a reasonable person would know and expect that the PII that was provided to Maximus by Mr. Brickman and the class members was provided in confidence and with the explicit understanding that Maximus would take all necessary precautions to protect the PII from unauthorized disclosure or dissemination to the public or any unauthorized third parties.

190. Maximus voluntarily received in confidence Mr. Brickman's and class members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

191. Due to Maximus's failure to prevent, detect, and avoid the Data Breach from occurring by following best information security practices to secure Mr. Brickman's and class members' PII, Mr. Brickman's and class members' PII was disclosed and misappropriated to the

public and unauthorized third parties beyond Mr. Brickman's and class members' confidence, and without their express permission.

192. But for Maximus's disclosure of Mr. Brickman's and class members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and/or used by unauthorized third parties.

193. The Data Breach was the direct and legal cause of the theft of Mr. Brickman's and class members' PII, as well as the resulting damages.

194. The injury and harm Mr. Brickman and class members suffered was the reasonably foreseeable result of Maximus's unauthorized disclosure of Mr. Brickman's and class members' PII.

195. Maximus knew its computer systems and technologies for accepting, securing, and storing Mr. Brickman's and class members' PII had serious security vulnerabilities because Maximus failed to observe even basic information security practices or correct known security vulnerabilities.

196. As a direct and proximate result of Maximus's breaches of confidence, Mr. Brickman and class members have been injured and were damaged as discussed herein and as will be proven at trial.

197. As a direct and proximate result of Maximus's breach of confidence, Mr. Brickman and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on DEA number

monitoring, credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Maximus, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT V

BREACH OF CONTRACT

(On behalf of Plaintiff and the Nationwide Class or, in the alternative, on behalf of Plaintiff and the Florida Subclass)

198. Mr. Brickman repeats the allegations in paragraphs 1 – 137 of this Complaint, as if fully alleged herein.

199. When Maximus and the state of Ohio entered into the Contract to provide services related to the credentialing and tax verification of Medicaid Providers, they intended to directly provide benefits to Mr. Brickman and class members.

200. As a result, Maximus received taxpayer funds and was required to be provided Mr. Brickman's and class members' PII, which it was obligated to keep confidential.

201. Upon information and belief, the Contract between Maximus and the Department of Administrative Services on behalf of ODM incorporated General Terms and Conditions,[33] including a provision governing confidentiality, which provided that "the Contractor [i.e., Maximus] also must treat as confidential materials such as . . . files containing personal information about individuals . . . such as personnel records, tax records, and so on, court and administrative

[33] A copy of these General Terms & Conditions are attached as part of Exhibit B, the Request for Proposals for Contract 0A1258 (the Contract that was ultimately awarded to Maximus).

records related to pending actions, any material to which an attorney-client, physician-patient, or similar privilege may apply, and any documents or records excluded by Ohio law from public record disclosure requirements." *See* Exhibit B, pp. 63-64.

202. This provision further provides that "[i]nformation . . . about people that is personal in nature, such as medical records, addresses, phone numbers, social security numbers, and similar things are . . . sensitive in nature and may not be disclosed or used in any manner except as expressly authorized in this contract." And it provides that "the Contractor must treat such information as Confidential Information whether it is available elsewhere or not." *Id.* at 64.

203. The provision further emphasized Maximus's obligations to keep Mr. Brickman's and class members' PII confidential: "The Contractor may not disclose any Confidential Information to third parties and must use it solely to do the project. . . The Contractor will be liable for the disclosure of such information, whether the disclosure is intentional, negligent, or accidental . . . ." *Id.*

204. Because the Contract was executed so that Maximus would provide services to Mr. Brickman and class members, and, *inter alia*, because the Contract specifically identified categories of PII for individuals such as Mr. Brickman and class members that Maximus must protect from unauthorized disclosure pursuant to the terms of the Contract, Mr. Brickman and class members were intended third-party beneficiaries under the contract(s) between the state of Ohio and Maximus.

205. Further demonstrating that Mr. Brickman and class members were intended third-party beneficiaries under the Contract, the Terms & Conditions impose a requirement that Maximus obtain "first and third party" "[c]yber liability" insurance to cover claims for, *inter alia*, "information theft" and "release of private information." *Id.* at 54.

206. Maximus violated the contracts by failing to employ reasonable and adequate

privacy practices and measures, leading to the disclosure of Mr. Brickman's and class members' PII for purposes not required or permitted under the contract(s) or the law.

207. As a direct and proximate result of Maximus's breach of contract, Mr. Brickman and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, DEA number monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Maximus, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

208. Additionally, because Mr. Brickman and class members continue to be third-party beneficiaries in the ongoing administration of the contract(s), and because damages may not provide a complete remedy for the breaches alleged herein, Mr. Brickman and class members are therefore entitled to specific performance of the contracts to ensure data security measures necessary to properly effectuate the contract(s) maintain the security of their PII from unlawful exposure.

COUNT VI

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT

Fla. Stat. § 501.201, *et seq.*

(On behalf of Plaintiff and the Florida Subclass)

209. Mr. Brickman repeats the allegations in paragraphs 1 – 137 of this Complaint, as if fully alleged herein.

210. The FDUTPA prohibits "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce . . ." Fla. Stat. § 501.204(1).

211. Maximus advertised, offered, or sold goods and services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

212. Maximus engaged in unfair, unconscionable acts or practices, and unfair or deceptive practices in the conduct of trade and commerce in violation of Fla. Stat. § 501.204(1), including by:

a. Failing to implement and maintain reasonable security and privacy measures to protect Mr. Brickman's and Florida Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing of the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Mr. Brickman's and Florida Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, Fl.

Stat. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that Maximus did not reasonably and adequately safeguard Mr. Brickman's and Florida Subclass members' PII; and

e. Omitting, suppressing, and concealing the material fact that Maximus did not comply with common law and statutory duties pertaining to the security and privacy of Mr. Brickman's and Florida Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, Fla. Stat. § 501.171(2).

213. Maximus's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Maximus's data security and ability to protect the confidentiality of PII.

214. Further, Maximus had knowledge and was aware that its security measures and protections of Mr. Brickman's and the class members' PII did not meet the accepted industry practices and standards for protection of PII.

215. Had Maximus disclosed to Mr. Brickman and Florida Subclass members that Maximus's data systems were not secure and, thus, vulnerable to attack, Maximus would have been forced to adopt reasonable data security measures and comply with the law. Instead, Maximus received, maintained, and compiled Mr. Brickman's and Florida Subclass members' PII as part of the services Maximus provided and for which it was compensated by the State of Ohio, without advising them that Maximus's data security measures were insufficient to maintain the safety and confidentiality of Mr. Brickman's and Florida Subclass members' PII. Accordingly, Mr. Brickman and Florida Subclass members acted reasonably in relying on Maximus's omissions, the truth of which they could not have discovered.

216. As a direct and proximate result of Maximus's unconscionable, unfair, and deceptive acts and practices, Mr. Brickman and Florida Subclass members have suffered and will continue to suffer injury, ascertainable losses of money and property, and monetary and non-monetary damages; loss of value of their PII; and an increased risk of fraud and identity theft.

217. Mr. Brickman and Florida Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

REQUEST FOR RELIEF

WHEREFORE, Mr. Brickman, individually and on behalf of all class members proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Maximus as follows:

1) For an Order certifying the Nationwide Class and the Florida Subclass, as defined herein, and appointing Mr. Brickman and Mr. Brickman's counsel to represent the Class as alleged herein;
2) For injunctive and other equitable relief as is necessary to protect the interests of Mr. Brickman and Class Members;
3) For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;
4) For an award of statutory damages and punitive damages, as allowed by law in an amount to be determined;
5) For an award of restitution or disgorgement, in an amount to be determined;
6) For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

7) For prejudgment interest on all amounts awarded; and

8) Such other and further relief as the Court may deem just and proper.

Respectfully Submitted,

DWORKEN & BERNSTEIN

Dated: September 28, 2021

s/ Frank A. Bartela

Frank A. Bartela, Esq. (#0088128)
fbartela@dworkenlaw.com
Nicole T. Fiorelli, Esq. (#0079204)
nfiorelli@dworkenlaw.com
Patrick J. Perotti, Esq. (#0005481)
pperotti@dworkenlaw.com
60 South Park Place
Painesville, Ohio 44077
Tel.: (440) 352-3391
Fax: (440) 352-3469

Andrea R. Gold, Esq.*
agold@tzlegal.com
Mark A. Clifford, Esq.*
mclifford@tzlegal.com
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Tel.: (202) 973-0900
Fax: (202) 973-0950

Counsel for Plaintiff Brickman and the Proposed Class

*Admitted *pro hac vice*

JURY DEMAND

Mr. Brickman, on behalf of himself and the Class of all others similarly situated, hereby demands a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Respectfully Submitted,

DWORKEN & BERNSTEIN

Dated: September 28, 2021

s/ Frank A. Bartela
Frank A. Bartela, Esq. (#0088128)
fbartela@dworkenlaw.com
Nicole T. Fiorelli, Esq. (#0079204)
nfiorelli@dworkenlaw.com
Patrick J. Perotti, Esq. (#0005481)
pperotti@dworkenlaw.com
60 South Park Place
Painesville, Ohio 44077
Tel.: (440) 352-3391
Fax: (440) 352-3469

Andrea R. Gold, Esq.*
agold@tzlegal.com
Mark A. Clifford, Esq.*
mclifford@tzlegal.com
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Tel.: (202) 973-0900
Fax: (202) 973-0950

Counsel for Plaintiff Brickman and the Proposed Class

*Admitted *pro hac vice*

CERTIFICATE OF SERVICE

I hereby certify that on September 28, 2021, a copy of the foregoing *First Amended Class Action Complaint* was filed electronically. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic filing receipt.

/s/ Frank A. Bartela
Frank A. Bartela, Esq. (#0088128)
DWORKEN & BERNSTEIN CO., L.P.A.

One of the Attorneys for Plaintiff